WHAT IS CLAIMED IS:

1. A method of protecting digital data, the method comprising:

separating the digital data into a plurality of data packets;

generating media encryption and decryption keys;

encrypting each of the data packets with one of the media encryption keys ;

generating a pair of protection encryption and decryption keys for each of the media encryption and decryption keys;

encrypting each one of the media decryption keys with a protection encryption key; and

storing the encrypted data packets, the encrypted media decryption keys, and the protection decryption keys.

2. The method of Claim 1, wherein the media encryption and decryption keys comprise two pairs of audio encryption and decryption keys, and wherein encrypting each of the data packets comprises encrypting each data packet such that no two time-successive packets are encrypted with the same audio encryption key.

3. The method of Claim 2, wherein:

storing the encrypted data packets, the two pairs of encrypted media decryption keys, and the two pairs of protection decryption keys comprises storing data on a removable medium;

one pair of protection encryption and decryption keys is reused across a plurality of removable media; and

one pair of protection encryption and decryption keys is unique to the removable medium.

4. A method of protecting digital audio content on a removable storage medium for use in a computing device, the method comprising:

generating at least one pair of audio encryption and decryption keys, such that for each audio encryption key there is a corresponding audio decryption key;

encrypting audio data with the at least one audio encryption key;

generating a pair of protection encryption and decryption keys for each of the decryption keys such that for each protection encryption key there is a corresponding protection decryption key;

encrypting the at least one audio decryption key with at least one protection encryption key;

storing the encrypted audio data on the removable medium;

storing the at least one encrypted audio decryption key on the removable medium; and

storing the at least one protection decryption key on the removable medium.

5. The method of Claim 4, wherein each audio encryption key is identical to its corresponding decryption key.

6. The method of Claim 4, wherein each pair of protection encryption and decryption keys comprises a public/private key pair.

7. The method of Claim 4, wherein:

the at least one pair of protection encryption and decryption keys comprises two pairs of keys;

one pair of protection encryption and decryption keys is reused across a plurality of removable media; and

one pair of protection encryption and decryption keys is unique to a removable medium.

8. The method of Claim 4, wherein storing the at least one protection decryption key comprises incorporating it into at least one decryption software module.

9. The method of Claim 4, wherein the removable storage medium is an optical medium, compact disc, or digital video disc.

10. The method of Claim 4, wherein:

the audio data comprises a plurality of discrete packets of audio data; and

the at least one pair of audio encryption and decryption keys comprises at least two pairs of audio encryption and decryption keys; and

wherein encrypting the audio data comprises encrypting each packet of the audio data so that every audio encryption key is used to encrypt at least one packet.

11. The method of Claim 4, further comprising:

storing unencrypted audio data on the removable medium, the unencrypted audio data formatted to be read by an audio media player; and

protecting the removable media so that the unencrypted audio data cannot be read by a computer.

12. The method of Claim 8, further comprising:

generating an access file describing allowed types of access to the encrypted audio data;

associating the access file with an identifier such that the access file cannot be read unless the associated identifier is present on the removable medium; and

storing the identifier on the removable medium, such that the identifier cannot be copied to another removable medium; and

wherein the at least one decryption software module cannot be used unless the access file can be read.

13. The method of Claim 12, wherein associating the access file with the identifier comprises:

generating a symmetric access file encryption key using the identifier as a seed; and

encrypting the access file with the encryption key.

14. The method of Claim 12, wherein associating the access file with the identifier comprises encrypting the access file along with a copy of the identifier and wherein the at least one decryption software module is configured so that it cannot decrypt the encrypted audio data unless after decrypting the access file and identifier, the module determines that the newly-unencrypted identifier matches the identifier previously stored on the removable medium.

15. A method of creating a protected audio storage medium, the method comprising:

storing digital audio data on the audio storage medium;

creating a first session on the medium, the first session containing audio data stored according to a first audio data storage format, the first session being readable

by an electronic device configured to read audio data stored according to the first audio storage format;

including on the first session at least one digital rights management license describing allowed uses for the audio data;

including on the first session digital rights management software;

encrypting the audio data on the first session so that the digital rights management software does not grant access to the digital audio data stored on the audio storage medium unless the digital rights management software determines that a requested access complies with the allowed uses described in the at least one digital rights management license;

creating a second session on the medium, the second session containing audio data stored according to a second audio data storage format, the audio data representing the same audio data contained on the first session and being readable by an audio player associated with a computing device configured to read audio data stored according to the second audio storage format; and

protecting the audio data contained on the second session so that the electronic device cannot access the audio data stored in the second session.

16. The method of Claim 15, wherein encrypting the audio data comprises:

separating the audio content into packets of audio data;

encrypting the packets;

storing the encrypted packets to the medium;

storing at least one audio decryption key on the medium such that the digital rights management software, when executed on a computer, uses the at least one decryption key to decrypt the packets and allows access to the audio.

17. The method of Claim 16, wherein encrypting the audio data further comprises:

creating at least two audio encryption keys;

for every audio encryption key, encrypting at least one packet with that key;

encrypting every packet with the at least two audio encryption keys; and

wherein the at least one audio decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

18. The method of Claim 17, wherein the audio encryption keys are symmetric, and wherein storing the decryption keys comprises:

generating at least one protection encryption key for each of the at least two audio encryption keys;

encrypting each audio encryption key with an associated protection encryption key;

storing the at least one encrypted audio encryption key on the medium, to serve as decryption keys; and

storing at least one protection decryption key on the medium, such that the protection decryption keys decrypt the at least one audio encryption key.

19. The method of Claim 18, wherein:

the at least one protection encryption key comprises a generic protection decryption key and a unique protection encryption key; and

the at least one protection decryption keys comprises a generic protection decryption key and a unique protection decryption key.

20. The method of Claim 19, wherein storing the protection decryption keys comprises integrating them inside the digital rights management software.

21. The method of Claim 20, wherein the digital rights management software is made tamper-resistant.

22. The method of Claim 21, additionally comprising:

placing a binding identifier on the medium, such that the binding identifier cannot be copied if the contents of the medium are duplicated on another medium;

associating the at least one digital rights management license with the binding identifier; and

wherein the digital rights management software does not allow access to the encrypted audio data unless the proper associated unique identifier is present on the medium.

23. The method of Claim 22, wherein associating the license with the binding identifier comprises encrypting the at least one license and a copy of the binding identifier together and including this encrypted file on the medium; and

wherein the digital rights management software does not allow access to the encrypted audio data based on rules described in the encrypted license unless the associated copy of the binding identifier, once decrypted, matches the binding identifier present on the medium.

24. The method of Claim 22, wherein associating the license with the binding identifier comprises:

using the binding identifier as a seed to create a license encryption key; and

encrypting the at least one license with the encryption key; and

wherein the digital rights management software is configured make a determination of whether the software will allow access to the encrypted audio data by using the binding identifier to create a decryption key, and then decrypting the at least one license.

25. The method of Claim 15, wherein the audio data on the first session comprises a plurality of separate audio recordings;

wherein the at least one digital rights management license comprises a plurality of digital rights management licenses; and

wherein at least one of the plurality of digital rights management licenses describes allowed uses for a specific track.

26. The method of Claim 15, wherein the medium is a compact disc.

27. A protected audio compact disc, comprising:

a first session, readable by an audio compact disc player;

audio data stored on the first session and protected so that the audio data on the first session cannot be decoded into a renderable media presentation by an optical media drive;

a second session, readable by an optical media drive;

at least one digital rights management license, written to the second session, and describing allowed uses for encrypted digital audio data;

digital rights management software, stored on the second session;

audio data stored on the second session, the second session audio data representing the same audio contained on the first session, and encrypted so that a

computing device executing the digital rights management software will not allow access to the second session audio data unless the computing device determines that the access is in compliance with the allowed uses described in the at least one digital rights management license; and

at least one decryption key, stored on the second session, such that the digital rights management software is configured to decrypt the encrypted digital audio data using the decryption key.

28. The compact disc of Claim 27, wherein the encrypted audio content comprises a plurality of encrypted packets of audio data.

29. The compact disc of Claim 28, wherein the plurality of encrypted packets are encrypted with a plurality of encryption keys, and wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

30. The compact disc of Claim 29, wherein the at least one decryption key is integrated inside the digital rights management software.

31. The compact disc of Claim 30, wherein the digital rights management software is tamper-resistant.

32. The compact disc of Claim 31, additionally comprising:

a binding identifier, stored on the compact disc such that the binding identifier cannot be copied if the contents of the compact disc are duplicated on another compact disc; and

wherein the at least one digital rights management license is associated with the binding identifier so that the digital rights management software does not allow access to the encrypted audio data unless the proper associated binding identifier is present on the compact disc.

33. The compact disc of Claim 32, wherein:

the at least one license and a copy of the binding identifier are encrypted together; and

the digital rights management software does not allow access to the encrypted audio data based on rules described in the encrypted license unless the associated

copy of the binding identifier, once decrypted, matches the binding identifier present on the disc;

and further comprising a file, stored on the second session on the compact disc, containing encrypted versions of the binding identifier and the at least one digital rights management license.

34. The compact disc of Claim 32, wherein:

the license is encrypted using an encryption key created by using the binding identifier found on the compact disc as a seed; and

the digital rights management software is configured make a determination of whether the software is permitted to allow access to the encrypted audio data by using the binding identifier to create a decryption key, and then decrypting the at least one license

35. The compact disc of Claim 27, wherein the audio data on the second session comprises a plurality of separate audio recordings;

wherein the at least one digital rights management license comprises a plurality of digital rights management licenses; and

wherein at least one of the plurality of digital rights management licenses describes allowed uses for a specific audio recording.

36. The compact disc of Claim 35, wherein the plurality of digital rights management licenses contains a license describing uses for a plurality of audio recordings written on the second session in addition to the at least one license that describes uses for a specific audio recording.

37. The compact disc of Claim 27, further comprising at least one validation code associated with the digital rights management software and written on the compact disc, wherein the at least one code represents a cryptographically-signed hash of a canonical representation of at least one section of the digital rights management software code, and wherein the digital rights management software is configured to detect tampering or replacement of the at least one section of code at the time the code is executed by performing a runtime hash of the at least one section of code and comparing the runtime hash to the stored cryptographically-signed hash.

38. The compact disc of Claim 27 further comprising protected playback software, written to the compact disc, the playback software configured to be copied to a storage device to play the audio data.

39. A system for protecting audio content, the system comprising:

a computing device;

at least one audio content file, stored on the computing device;

at least one digital rights management license, stored on the computing device, describing allowed uses for the at least one digital audio content file;

digital rights management software, stored on the computing device, configured to allow access to the at least one audio content file only if the access is in compliance with the uses described in the at least one digital rights management license; and

wherein the at least one audio content file, the at least one digital rights management license, and the digital rights management software were installed on the computing device from a digital audio medium.

40. The system of Claim 39, further comprising:

a hard drive, coupled to the computing device;

an identifier, stored on the hard drive; and

wherein the at least one digital rights management license is associated with a hard drive identifier so that the digital rights management software does not allow access to the at least one audio content file unless the identifier with which the at least one license is associated is the same as the identifier stored on the hard drive.

41. The system of Claim 39, wherein the digital rights management software comprises a generic module and a unique module.

42. The system of Claim 39, further comprising:

at least one validation code, corresponding to at least one predetermined software module and computed prior to the software module being stored on the computing device; and

validation software, configured to determine if predetermined software modules is trusted by computing at least one checksum for at least one software

module in the system and comparing those checksums against the prior-computed validation code.

43. The system of Claim 42, wherein:

the at least one validation code is a cryptographically-signed hash of a canonically-ordered series of bytes from the at least one predetermined software module; and comparing checksums against the prior-computed validation code comprises:

decrypting the cryptographically-signed hash;

performing a hash on the at least one software module in the system; and

comparing the results of the two hashes to see if they match.

44. The system of Claim 39, wherein the audio medium is a compact disc.

45. A method of transferring digital audio data from a protected audio storage medium to a storage device on a computing device, the method comprising:

copying at least one encrypted audio file from the protected audio storage medium to the storage device, along with encryption keys that can be used to decrypt these files; and

copying at least one digital rights management license from the protected audio storage medium to the storage device, the digital rights management license describing types of access that are allowed for the at least one copied audio file;

wherein the copied digital rights management software is configured to allow access to the at least one copied audio file only if the access is in compliance with the types of access described in the at least one digital rights management license.

46. The method of Claim 45, further comprising:

determining whether the computing device has digital rights management software and secure playback software that are compatible with playing the at least one encrypted audio file; and

installing the compatible digital rights management software or secure playback software if the computing device does not have them.

47. The method of Claim 46, further comprising encrypting the at least one digital rights management license and wherein the copied digital rights management software does

not allow access to the at least one copied audio file unless the at least one digital rights license is decrypted.

48. The method of Claim 47, wherein encrypting the at least one digital rights management license comprises:

generating a binding identifier for the storage device;

storing the identifier on the storage device such that it is difficult to modify;

generating an encryption key using the binding identifier as a key; and

encrypting the at least one digital rights management license using the generated encryption key;

and wherein the digital rights management software is configured to create a decryption key for the at least one license using the binding identifier as a key.

49. The method of Claim 45, wherein the protected audio medium is a compact disc.

50. A method of playing digital audio data stored on a protected digital audio medium using digital rights management software on a computing device, the method comprising:

determining if the at least one digital rights management license on the digital audio medium allows playback of the digital audio data stored thereon;

decrypting encrypted digital audio data contained on the protected digital audio medium in response to said determining; and

causing the decrypted digital audio data to be played on the computing device.

51. The method of Claim 50, wherein the protected digital audio medium is a compact disc.

52. The method of Claim 50, further comprising authenticating software stored on the computing device to verify that it has not been tampered with or modified.

53. The method of Claim 52, wherein the encrypted digital audio contained on the digital audio medium comprises a plurality of encrypted packets of audio data.

54. The method of Claim 53 wherein decrypting the digital audio contained on the digital audio medium comprises:

locating at least one audio decryption key on the digital audio medium; and

decrypting the packets of audio data using the at least one audio decryption key.

55. The method of Claim 54, wherein:

each of the at least one audio decryption keys is itself encrypted with a protection encryption key; and

the digital audio medium contains at least one protection decryption key which decrypts the encrypted audio decryption key;

and wherein locating the at least one decryption key on the digital audio medium comprises decrypting the at least one encrypted audio decryption key using the at least one protection decryption key.

56. The method of Claim 55, wherein:

the at least one protection encryption keys comprises a generic protection encryption key and a unique protection encryption key; and

the at least one protection decryption keys comprises a generic protection encryption key and a unique protection encryption key.

57. The method of Claim 55, wherein the at least one audio decryption keys are symmetric.

58. The method of Claim 55, further comprising:

generating a symmetric playback protection key; and

encrypting the at least one audio decryption key with the symmetric key;

and wherein decrypting encrypted audio further comprises decrypting the at least one encrypted audio decryption key prior to decrypting the packets of audio data.

59. The method of Claim 58, wherein playing the encrypted audio further comprises deleting the at least one audio decryption key and the decrypted packets of audio data from memory.

60. A method of transferring digital audio data from a protected digital audio storage media to an external device, the method comprising:

loading digital rights management software from the protected media;

retrieving a digital rights management license from the protected media;

determining that transfer of the digital audio data is allowed by the retrieved digital rights management license; and

transferring at least one audio file to the external device.

61. The method of Claim 60, wherein the protected media is a compact disc.

62. The method of Claim 60, further comprising authenticating software stored on the device to verify that the software has not been tampered with or modified and is trusted to protect against unauthorized copying of the files.

63. The method of Claim 60, wherein the external device is a compact disc burner.

64. The method of Claim 60, wherein the external device is a portable audio player.

65. The method of Claim 60, further comprising translating the at least one audio file into a format compatible with the external device.

66. The method of Claim 64, further comprising transferring digital rights management software and at least one digital rights management license from the protected audio media to the external device.

67. The method of Claim 66, wherein the external device contains digital rights management software and further comprising:

translating the at least one digital rights management license into a format compatible with the software on the external device; and

transferring the translated digital rights management license to the external device.

68. A medium readable by a computing device, the medium containing instructions which, when executed, perform the method comprising:

locating a digital rights management license on the medium;

determining if the license on the medium allows playback;

decrypting encrypted digital audio data contained on the medium; and

playing the decrypted audio data.

69. The medium of Claim 68, wherein the medium is a compact disc.

70. The medium of Claim 68, further comprising instructions which, when executed, perform the step of authenticating software stored on the computing device to verify that it has not been tampered with or modified.

71. The medium of Claim 70, wherein the encrypted audio data comprises encrypted packets of audio data.

72. The medium of Claim 71 wherein decrypting the audio data comprises:

locating a decryption key on the medium; and

decrypting the packets of audio data using the audio decryption key.

73. The medium of Claim 72, wherein:

the decryption key is itself encrypted with a protection encryption key;

the medium contains a protection decryption key which decrypts the encrypted audio decryption key; and

wherein locating the decryption key on the medium comprises decrypting the encrypted audio decryption key using the protection decryption key.

74. The medium of Claim 73, wherein:

the protection encryption keys comprises a generic protection encryption key and a unique protection encryption key; and

the protection decryption keys comprises a generic protection encryption key and a unique protection encryption key.

75. The medium of Claim 73, wherein the audio decryption keys are symmetric.

76. The medium of Claim 73, further comprising instructions which, when executed, perform the steps of:

generating a symmetric playback protection key;

encrypting the audio decryption key with the symmetric key; and

wherein decrypting encrypted audio further comprises decrypting the encrypted audio decryption key prior to decrypting the packets of audio data.

77. The medium of Claim 76, wherein playing the encrypted audio further comprises deleting the audio decryption key and the decrypted packets of audio data from memory.